UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MICHELLE BOYER, individually and on behalf of all others similarly situated, Plaintiff, v. ALLEGHENY HEALTH NETWORK, ALLEGHENY HEALTH NETWORK HOME MEDICAL EQUIPMENT LLC, ALLEGHENY HEALTH NETWORK HOME INFUSION LLC, and INTRASYSTEMS, LLC, Defendants.	Case No. _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Michelle Boyer ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendants Allegheny Health Network, Allegheny Health Network Home Medical Equipment LLC, Allegheny Health Network Home Infusion LLC (together, "AHN"), and IntraSystems, LLC ("IntraSystems" and, with AHN, "Defendants"), and complains and alleges upon personal knowledge as to herself and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard approximately 292,773 persons' (including Plaintiff's) personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, Social Security numbers, financial account numbers, health insurance identification numbers and other health insurance information, and treatment information including diagnoses,

provider information, treatments/procedures, dates of service, prescription information, and medical device serial numbers.

2. Allegheny Health Network is an integrated health network with 14 hospitals and over 250 other locations, concentrated in western Pennsylvania. It is the parent company of Defendants Allegheny Health Network Home Medical Equipment LLC and Allegheny Health Network Home Infusion LLC. IntraSystems is an IT consulting and service provider that provides services to AHN.

3. Between approximately October 14, 2024, and November 19, 2024, an unauthorized third party gained access to IntraSystems' network systems and accessed and acquired files containing the PII/PHI of AHN's patients, including Plaintiff and Class members (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to, or contracting with companies that failed to, implement and maintain reasonable security procedures and practices to protect their patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach, which occurred between approximately October 14, 2024, and November 19, 2024.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Michelle Boyer

7. Plaintiff Michelle Boyer is a citizen of Pennsylvania.

8. Plaintiff received healthcare services or related services from AHN. As a condition of providing healthcare or related services to Plaintiff, AHN required Plaintiff to provide it with her PII/PHI.

9. AHN used systems and services provided by IntraSystems to store, transfer, and maintain Plaintiff's PII/PHI.

10. Based on representations made by AHN, Plaintiff believed Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to AHN in connection with obtaining healthcare or related services provided by AHN.

11. At all relevant times, Defendants stored and maintained Plaintiff's PII/PHI on their network systems, including the systems affected in the Data Breach.

12. Plaintiff received a letter from AHN notifying her that her PII/PHI was affected in the Data Breach.

13. Had Plaintiff known that Defendants do not adequately protect the PII/PHI they collect and maintain, she would not have agreed to provide AHN with her PII/PHI or obtained healthcare or related services from AHN.

14. As a result of her PII/PHI being accessed and stolen in the Data Breach, Plaintiff spent time and effort freezing her credit. In addition, she has experienced a sizeable increase in the number of spam calls, text messages, and emails she receives; since the breach, she receives approximately five spam calls, two spam emails, and one to two spam text messages every day.

15. As a direct result of the Data Breach, Plaintiff has suffered other injury and damages including, *inter alia*, a substantially increased and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; and deprivation of the value of her PII/PHI.

Defendant Allegheny Health Network

16. Defendant Allegheny Health Network is a Pennsylvania nonprofit corporation with its principal place of business located at 120 Fifth Avenue, Suite 2900, Pittsburgh, PA 15222.

Defendant Allegheny Health Network Home Medical Equipment LLC

17. Defendant Allegheny Health Network Home Medical Equipment LLC is a Pennsylvania corporation with its principal place of business located at 463 Napor Boulevard, Suite 103, Pittsburgh, PA 15205.

Defendant Allegheny Health Network Home Infusion LLC

18. Defendant Allegheny Health Network Home Infusion LLC is a Pennsylvania corporation with its principal place of business located at 1305 South Main Street, Meadville, PA 16335.

Defendant IntraSystems, LLC

19. Defendant IntraSystems, LLC is a Massachusetts corporation with its principal place of business located at 35 Braintree Hill Office Park, Suite 403, Braintree, MA 02184. It may be served through its registered agent: Corporation Service Company, 84 State Street, Boston, MA 02109.

JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

21. This Court has general personal jurisdiction over Defendant IntraSystems, LLC because it is a Massachusetts corporation and maintains its principal place of business in Massachusetts.

22. The Court has personal jurisdiction over Defendants Allegheny Health Network, Allegheny Health Network Home Medical Equipment LLC, and Allegheny Health Network Home Infusion LLC because they transact business in this State and contract for goods or services in this State.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant IntraSystems' principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

24. AHN is an integrated health system that serves 29 Pennsylvania counties and portions of New York, Ohio, and West Virginia. AHN provides a comprehensive range of healthcare services at 14 hospitals and over 300 care locations, as well as home medical equipment and home infusion therapy. Allegheny Health Network Home Medical Equipment LLC and Allegheny Health Network Home Infusion LLC are subsidiaries of Allegheny Health Network.[1]

25. IntraSystems is an "IT consulting company, managed services provider, and systems integrator that specializes in the deployment, management, and delivery of IT infrastructure, managed services, help desk services, cybersecurity services and assessments, virtualization services, security, and cloud solutions."[2] IntraSystems provides IT products or services to AHN.

26. In the regular course of its business, AHN collects and maintains the PII/PHI of its current and former patients, including Plaintiff and Class members. AHN required Plaintiff and Class members to provide it with their PII/PHI as a condition of providing healthcare or related services. AHN then shared Plaintiff and Class members' PII/PHI with IntraSystems in connection with using IntraSystems' services or products.

27. AHN provides its patients with a Notice of Privacy Practices ("Privacy Notice"). The Privacy Notice describes the way AHN may use and disclose its patients' PII/PHI.

---

[1] *See* Ionut Arghire, *430,000 Impacted by Data Breaches at New York, Pennsylvania Healthcare Organizations*, SEC. WEEK (Feb. 7, 2025), https://www.securityweek.com/430000-impacted-by-data-breaches-at-new-york-pennsylvania-healthcare-organizations/.

[2] *About IntraSystems*, INTRASYSTEMS, https://www.intrasystems.com/about-intrasystems/ (last accessed Feb. 11, 2025).

28. In the Privacy Notice, AHN promises its patients it will "respect your right to privacy and function to ensure your confidentiality by following federal and state laws concerning protected health information." AHN represents it is "committed to protecting the privacy of your protected health information." It claims to "understand that medical information about you and your health is important to you."

29. AHN admits it is "required by applicable federal and state laws to maintain the privacy" of its patients' PII/PHI.

30. AHN states in the Privacy Notice that it will use or disclose PII/PHI only for specified purposes, including for treatment, payment, and health care operations. It also states that when it shares PII/PHI with a business associate, the business associate must agree in writing to protect the confidentiality of PHI.

31. AHN promises that "uses and disclosures of PHI not covered by this Notice or applicable laws will be made only with" patients' written authorization.

32. AHN also promises patients it will inform them if their PII/PHI is affected in a data breach.

33. IntraSystems represents itself as being committed "to the highest levels of security and data protection."[3] IntraSystems claims it "safeguards organizations from data breaches and cyberattacks with cutting-edge cybersecurity solutions," including "assessments, email security, threat detection, IT health checks, and more."[4]

[3] *Id.*
[4] *Cybersecurity Services*, INTRASYSTEMS, https://www.intrasystems.com/cybersecurity/ (last accessed Feb. 11, 2025).

34. IntraSystems encourages users of its healthcare-related services to "[t]rust IntraSystems when privacy, security, and reliability matter most."[5] IntraSystems represents that it "Protect[s] Sensitive Patient Data with Advanced Encryption and Security Protocols."[6]

35. Plaintiff and Class members are current and former patients of AHN who entrusted AHN with their PII/PHI in exchange for healthcare services and whose PII/PHI was in turn shared with IntraSystems.

The Data Breach

36. Beginning on or about October 14, 2024, an unauthorized third party gained access to certain AHN computer systems hosted, managed, or secured by IntraSystems and accessed and acquired files containing the PII/PHI of Plaintiff and Class members. AHN did not discover the Data Breach until approximately November 19, 2024. The PII/PHI accessed and acquired in the Data Breach includes names, dates of birth, addresses, Social Security numbers, financial account numbers, health insurance identification numbers and other health insurance information, and treatment information including diagnoses, provider information, treatments/procedures, dates of service, prescription information, and medical device serial numbers.

37. While AHN learned of the Data Breach on or about November 19, 2024, it waited until approximately January 17, 2025, nearly two months after discovering the Data Breach and over three months after the Data Breach began, to begin notifying its patients affected in the Data Breach that their PII/PHI had been compromised.

38. Defendants' failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited

[5] *Healthcare Services*, INTRASYSTEMS, https://www.intrasystems.com/it-healthcare/ (last accessed Feb. 11, 2025).
[6] *Id.*

those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII/PHI

39. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected and maintained was a target for malicious actors. Indeed, AHN acknowledges in its Privacy Notice that it will inform patients if a data breach occurs, and IntraSystems advertises its data breach-related security services. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyberattacks that they should have anticipated and guarded against.

40. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[7]

41. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[8] This is an

[7] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[8] *See 2024 Breach Barometer*, PROTENUS 2, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-

increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[9]

42. PII/PHI is a valuable property right.[10] The value of PII/PHI as a commodity is measurable.[11] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

43. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last accessed Dec. 13, 2024).

[9] *See id*.

[10] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[11] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[12] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[13] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

44. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[14] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[15]

45. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[16] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[17]

46. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[19]

---

[14] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[15] *Id.*
[16] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[17] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[18] Steager, *supra* note 14.
[19] *Id.*

47. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

48. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

49. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[21] [22]

50. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying

[20] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[21] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Dec. 13, 2024).

[22] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[23]

51. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[24]

52. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[25] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[26] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [27] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[28]

---

[23] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[24] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Dec. 13, 2024).

[25] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[26] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 17.

[27] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Dec. 13, 2024).

[28] *Id*.

53. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [29]

54. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[30]

[29] *See* Dixon & Emerson, *supra* note 25.
[30] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

55. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and Class Members

56. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, theft, and publication of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

57. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

58. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons whose personally identifiable information and personal health information was accessed by and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

59. Plaintiff also brings this action on behalf of herself and all members of the following subclass (the "Pennsylvania Subclass"):

> All citizens of Pennsylvania whose personally identifiable information and personal health information was accessed by and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

60. Excluded from the Class are Allegheny Health Network and its affiliates, parents, subsidiaries, officers, agents, and directors; IntraSystems, LLC and its affiliates, parents, subsidiaries, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge.

61. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

62. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. AHN has reported to the U.S. Department of Health and Human Services that the Data Breach affected approximately 292,773persons.[31]

63. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had a duty not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

[31] *Cases Currently Under Investigation*, DEP'T HEALTH & HUM. SERVS. (Jan. 17, 2025), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

e. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

f. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

64. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

65. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

66. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

67. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

68. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

69. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

70. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

71. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII/PHI.

72. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure

systems. Defendants knew, or should have known, of the many data breaches that targeted companies that collect and store PII/PHI in recent years.

73. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

74. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

75. Plaintiff and Class members had no ability to protect their PII/PHI that was, or remains, in Defendants' possession.

76. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

77. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendants'

failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, adopting, implementing, and maintaining appropriate security measures.

78. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF FIDUCIARY DUTY
Against AHN Only

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. As a condition of obtaining services from AHN, Plaintiff and Class members gave AHN their PII/PHI in confidence, believing that AHN would protect that information. Plaintiff and Class members would not have provided AHN with this information had they known it would not be adequately protected. AHN's acceptance, use, and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between AHN and Plaintiff and

Class members. In light of this relationship, AHN must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

81. AHN has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by, among other things, failing to, or contracting with third parties that failed to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected, utilized, and maintained.

82. As a direct and proximate result of AHN's breach of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT
Against AHN Only

83. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

84. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with AHN.

85. Pursuant to these implied contracts, Plaintiff and Class members paid money to AHN (directly or through their insurance) and provided AHN with their PII/PHI. In exchange, AHN agreed to, among other things, and Plaintiff and Class members and AHN mutually understood that AHN would: (1) provide healthcare or related services to Plaintiff and Class members; (2) use Plaintiff's and Class members' PII/PHI to facilitate providing healthcare services to Plaintiff and Class members; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (4) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations, industry standards, and AHN's representations regarding its security and privacy practices

86. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and AHN, on the other hand. Indeed, as set forth *supra*, AHN recognized the importance of data security and the privacy of its patients' PII/PHI in, *inter alia*, its Privacy Notice. Plaintiff and Class members and AHN mutually understood and agreed that the healthcare or related services AHN would provide to Plaintiff and Class members included AHN's protection of Plaintiff's and Class members' privacy and PII/PHI. Had Plaintiff and Class members known that AHN would not adequately protect its patients' and former patients' PII/PHI, they would not have paid for or obtained healthcare or related services from AHN.

87. Plaintiff and Class members performed their obligations under the implied contract when they provided AHN with their PII/PHI and paid for healthcare or related services from AHN, expecting that their PII/PHI would be protected.

88. AHN breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

89. AHN's breach of its obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

90. Plaintiff and all other Class members were damaged by AHN's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

91. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

92. This claim is pleaded in the alternative to the breach of implied contract claim.

93. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid to AHN for healthcare or related services, which AHN in turn used to pay IntraSystems for its services, with an implicit understanding that Defendants would use some of these payments to protect the PII/PHI they collect, store, and use to provide health care.

94. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing and payment services and other aspects of Defendants' business.

95. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

96. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

97. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL")
73 P.S. §§ 201-1–201-9.3
On Behalf of the Pennsylvania Subclass Against AHN Only

98. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

99. Plaintiff brings this claim individually, and on behalf of the Pennsylvania Subclass, only against Defendant Allegheny Health Network.

100. AHN performs services in the Commonwealth of Pennsylvania.

101. Plaintiff, Class members, and AHN are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

102. AHN's healthcare and other services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

103. AHN obtained Plaintiff's and Class members' PII/PHI in connection with the healthcare and other services that AHN performed.

104. AHN engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure its patients' and former patients' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards.

105. AHN makes explicit statements to its patients that their PII/PHI will remain private.

106. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). AHN's failure to adequately protect Plaintiff and Class members' PII/PHI while holding out that it would adequately protect the PII/PHI falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

107. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, AHN's failure to adopt reasonable practices in protecting and safeguarding its patients' PII/PHI will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for AHN's practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

108. As a result of AHN's violations of the UTPCPL, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting

to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in AHN's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

109. Pursuant to 73 P.S. § 201-9.2(a), Plaintiff seeks actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiff also seeks costs, expenses, and reasonable attorney fees.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 12, 2025

Respectfully submitted,

/s/ *David Pastor*
David Pastor (BBO 391000)
PASTOR LAW OFFICE PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617-742-9700
Fax: 617-742-9701
dpastor@pastorlawoffice.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
Cook County Attorney No. 38957
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff Michelle Boyer

**Pro hac vice* forthcoming